UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,065	07/26/2001	Florian Oelmaier	3118	6076

7590 12/01/2004

Ralph H. Dougherty
DOUGHERTY & CLEMENTS LLP
Two Fairview Center
6230 Fairview Road, Suite 400
Charlotte, NC 28210

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/787,065	OELMAIER ET AL.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-18 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-18 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 12 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5/21/2001.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12, 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney et al (6351813 B1).

With respect to Claim 1, the limitation of "a device (10) for supplying output data (14) in reaction to input data comprising an electronic circuit (16) for executing an algorithm so as to generate the output data (12) on the basis of the input data (14)" on column 1, lines 59-67; and "a unit (18) for detecting operational data of the electronic circuit (16) which are influenced by an operation of said electronic circuit (16) when said electronic circuit (16) executes the algorithm, the operational data depending on the input data" on column 2, lines 36-41; and "said operational data detection unit (18) being coupled to the electronic circuit (16) in such a way that the detected operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit (16), for generating the output data (12), whereby the authenticity of the device (10) is determined on the basis of the output data" on column 3, lines 30-46. The smart card represents the electronic circuit while the smartcard reader represents the unit for detecting operational data of the electronic circuit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the smartcard represent the electronic circuit because a smart card has a built-in electronic circuit though which output data is generated based on its input data.

With respect to Claim 2, the limitation of "wherein the operational data are selected from the group comprising time data and power data" is met on column 8, lines 47-52, 62-64. For the smartcard to operate it needs either an internal or external power source. Without a power source input to the smartcard, it would be inoperable.

With respect to Claim 3, the limitation of "wherein the electronic circuit (16) and the detection unit (18) are integrated as a unit" is met on column 6, lines 45-49.

With respect to Claim 4, the limitation of "which is contained in a smart card or in a PC card" is met on column 3, lines 42-44.

With respect to Claim 5, the limitation of "wherein the electronic circuit (16) is arranged so as to execute an cryptoalgorithm" is met on column 3, lines 61-67 and on column 4, lines 1-4.

With respect to Claim 6, the limitation of "wherein the electronic circuit (16) is arranged so as to execute a check sum algorithm" is met on column 4, lines 66-67, column 5, lines 1-7.

With respect to Claim 7, the limitation of "wherein the cryptoalgorithm is a multi-step algorithm, the operational data of one algorithm step being used as input data for the subsequent algorithm step" is met on column 3, lines 61-67 and on column 4, lines 1-4.

With respect to Claim 8, the limitation of "wherein the electronic circuit (16) is arranged so as to stop the operation after a predetermined execution time during execution of the algorithm and wherein the detection unit (18) is arranged so as to feed operational data into the algorithm at said predetermined execution time" is met on column 8, lines 62-66.

With respect to Claim 9, the limitation of "wherein the algorithm is of such a nature that it will first randomize the input data (14), whereby the dependence of the operational data on the input data will be pseudo-random" is met on column 3, lines 64-67.

With respect to Claim 10, the limitation of "wherein the output data generated by the algorithm are only the operational data" on column 3, lines 30-46.

With respect to Claim 11, the limitation of "wherein the electronic circuit (16) comprises two sub-circuits (16a, 16b) which each execute a sub-algorithm, the first sub-algorithm being a test algorithm whose operational data are detected by the detection unit (18), and the second sub-algorithm being a cryptoalgorithm or a check sum algorithm, the operational data of the test algorithm being processed in the cryptoalgorithm" is met on column 3, lines 52-54, 64-67; column 4, lines 1-2, 66-67; column 5, lines 1-7; and column 7, lines 6-12.

With respect to Claim 12, the limitation of "wherein the second sub-circuit (16a) is arranged so as to execute the DES algorithm which comprises n steps, and wherein the first sub-circuit (16b) is arranged so as to execute a test algorithm which also comprises n steps, the input data being adapted to be fed into the first step of the DES algorithm as well as into the first step of the test algorithm, and data which are adapted to be fed into a further step of the DES algorithm being result data of the first step of the DES algorithm and operational data of the first step of the test algorithm, whereas a result of one step of the test algorithm is rejected" is met on column 5, lines 22-40.

With respect to Claim 16, the limitation of "wherein the operational data detection unit (18) comprises a pattern recognition algorithm so as to produce the operational data from power or time parameters of the electronic circuit (16)" is met on column 8, lines 57-61.

With respect to Claim 17, the limitation of "a method for checking the authenticity of a device to be tested in comparison with an examination device, the device to be tested and the examination device each comprising an electronic circuit (16) for executing an algorithm, which generates output data (12) on the basis of input data (14), and a unit (18) for detecting operational data which are influenced by an operation of the electronic circuit (16) and which depend on the input data, the operational data detection unit (18) of the device to be tested as well as of the examination device being coupled to the electronic circuit (16) in such a way that the operational data of the electronic circuit are used by the algorithm for producing the output

data" is similar to Claim 1 and hence has been rejected above. Further limitation of "selecting (40) input data; feeding (42) said input data into the device (10) to be tested" is met on column 7, lines 6-9; and "in the device to be tested executing the algorithm by the electronic circuit of the device to be tested, so as to generate the output data on the basis of the input data" is met on column 7, lines 9-13; and "detecting operational data of the electronic circuit, which are influenced by an operation of said electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data" is met on column 2, lines 36-41; and "said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit (16), so as to generate the output data (12)" is met on column 4, lines 2-9; and "feeding (42) the input data into the examination device (10)" is met on column 4, lines 2-4; and "in the examination device executing the algorithm by the electronic circuit of the examination device so as to generate the output data on the basis of the input data" on column 3, lines 61-67; and column 4, lines 1-2; and "detecting operational data of the electronic circuit, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit (16), so as to generate the output data (12)" is met on column 4, lines 2-9; and "comparing (44) the output data of the device to be tested with the output data of the examination device; and affirming (46) the authenticity of the device to be tested in comparison with the examination device if the output data correspond to one another, in such a way that authenticity will only be affirmed if the operational data of the device to be tested and of the examination device correspond to one another" is met on column 5, lines 36-45.

With respect to Claim 18, the limitation of "a method for encrypted transmission of information from a first to a second location, the second location being remote from the first location" is met on column 6, lines 50-53 and Fig. 11; and " producing (50) a random word" is met on column 5, lines 45-47; and "feeding (52) the random word into a first device implemented according to one of the claims 1-16 and arranged at the first location" is met on column 6, lines 48-54; and "generating (54) the output data of the second device, which depend on the operational data of said first device, by executing an algorithm by the electronic circuit of said first device so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data" is met on column 5, lines 66-67; and on column 6, lines 1-23; and "encrypting (56) the information with the generated output data as a key" is met on column 6, lines 24-30, 34-37; and "transmitting (58) the encrypted information and the random word from said first location to said second location" is met on column 6, lines 40-44; and "feeding (62) the random word into a second device implemented according to one of the claims 1-16 and positioned at the second location; and "generating (64) the output data of the second device, which depend on the operational data of said second device, by executing the algorithm by the electronic circuit of said second device, so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said

electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data; and decrypting (66) the encrypted information making use of the output data of the second device as a key; and the decrypted information corresponding to the original information prior to encrypting if the operational data of the first device at the first location correspond to the operational data of the second device at the second location" is met on column 6, lines 44-49.

Claims 13, 14, 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney et al (6351813 B1) in view of Walsh et al (6144848).

With respect to Claim 13, Mooney et al meets the limitation of "wherein the operational data detection unit comprises a time measuring means (18a) for measuring the time which the electronic circuit (16) needs for executing a specific task" on column 8, lines 47-52, 62-64. Mooney et al however does not meet the following limitation.

The limitation of "a power measuring means (18b) for measuring the power consumed when said specific task is being executed" is met by Walsh et al in Claim 32.

It would have obvious to one of ordinary skill in the art to combine the teachings of Walsh et al within the system of Mooney et al because measuring the level of power consumed allows for the system to determine if/when to recharge the electronic circuit.

With respect to Claim 14, Mooney et al meets all the limitation except for the following limitation.

The limitation of "wherein the power measuring means (18b) comprises a resistor, a capacitor and an analog-digital converter for measuring the power consumed" is met by Walsh et al in Claim 33.

It would have obvious to one of ordinary skill in the art to combine the teachings of Walsh et al within the system of Mooney et al because measuring the level of power consumed allows for the system to determine if/when to recharge the electronic circuit.

With respect to Claim 15, Mooney et al meets the limitation of "wherein the time measuring means comprises an internal clock generator" on column 8, lines 47-52, 62-64.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

OTA